Maine State Government
Dept. of Administrative & Financial Services
Office of Information Technology (OIT)

Procedure for Secure ID Cards and Maintenance of the RSA Database

I. **Statement**

State agencies will comply with this standard when acquiring Secure ID cards. Security Coordinators will comply with this standard for maintaining accountability for Secure ID cards.

II. **Purpose**

The purpose of this standard operating procedure (SOP) is to govern the accountability and procedures for Secure ID cards.

III. **Guidelines**

A. Secure ID Program Administrator

1. Will maintain the overall supervision of this program and keep all procedures current and up to date.

2. Ensure that an adequate number of Secure ID cards are available to fulfill requests.

3. Maintain Security Coordinator list and distribute to Call Center specialist.

4. Ensure that this list is verified semi-annually with the agencies.

5. On a monthly basis provide Secure ID card holders list to each of the Security Coordinators for their perspective agencies.

6. Generate a monthly inactivity report for Contractor card holders greater than 120 days. Provide this list to the Security Coordinators and inform them that these cards will be disabled. Disable all 120 day or greater inactive Contractor card users.

B. Security Coordinator

1. The Security Coordinator will provide the Call Center with a request for the Secure ID card via an electronic form on http://footprints.state.me.us/footprints/rsa.html (if you have not been set up for this web site and would like to be, call 624-7700 and one of the Call Center staff can set you up with a

user name and password) or put a ticket in via the Footprints portal: https://footprints.state.me.us/footprints

2. Review end of month report to determine if a Secure ID card is needed for cards expiring and that all users are valid.

3. Upon notification from users that have been disabled, verify their status and contact the Call Center for placement into active status.

4. Notify Secure ID Program Administrator of any changes to Security Coordinator assignments.

5. If a contractor leaves the State, ensure that the agency completes a Delete User form, which is under the User Request project within Footprints.

C. Call Center Specialist

1. When the Call Center receives a Secure ID request, the request is to be completed according to the instructions located on the P: drive at oit-desktop on oit-teaqfsemc01/oit/sop/secureidsection.doc.

2. For users calling in that are unable to login and have verified that they have been disabled for inactivity due to multiple logon attempts, re-enable their login. If they have not logged into the system within 120 days or more, then have those users contact their Security Coordinator for re-activation of their card.

3. Disable accounts for those contractors that are no longer working for the State, as directed by the Agency.

IV. **Applicability**

This is intended to manage the process of acquiring and accountability of Secure ID cards for: Employees and Contractors of Agencies within the Executive Branch and semi-autonomous State Agencies.

V. **Responsibilities**

A. Agency Supervisor(s) or their designees will be responsible for approving the request for a Secure ID card and the cost of that card.

B. Security Coordinators, working with the Agency Supervisors will request online Secure ID cards for Contractors and all State Employees.

C. The Secure ID Program Administrator will ensure that all aspects of the Secure ID card program are followed in accordance with this policy.

VI. **Definitions**

A. Secure ID card: To access resources protected by the RSA SecurID system, users simply combine their secret Personal Identification Number (PIN) (something they alone know) with the token codes generated by their authenticators (something they have). The result is a unique, one-time-use passcode that is used to positively identify, or authenticate, the user, with “two-factor” authentication. If the code

is validated by the RSA SecurID system, the user is granted access to the protected resource. If it is not recognized, the user is denied access. NOTE: The acronym RSA stands for Rivest, Shamir, Adelman, the inventors of this encryption technique.

B. RSA Database: RSA Access Manager software is designed to enable organizations to manage large numbers of users while enforcing a centralized security policy that ensures compliance, protects enterprise resources from unauthorized access, and makes it easier for legitimate users to do their jobs.

C. Agency Supervisor(s): A Supervisor or Manager within the Agency who can grant authorization for the purchase of a Secure ID card and can grant an Employee use of a Secure ID card.

D. Semi-autonomous State Agency: An Agency created by an act of the Legislative Branch that is not a part of the Executive Branch. This term does not include the Legislative and Judicial Branches, Offices of the Attorney General, Secretary of State, State Treasurer, and Audit Department.

E. Security Coordinator: The person designated by the Agency to manage the ordering of new and expired Secure ID cards through a report sent to them each month from the Secure ID Program Administrator.

F. Call Center Specialist: The person at the Call Center who fulfills the requests submitted by the Security Coordinator or designated person.

G. Secure ID Program Administrator: The person at the Call Center who administers the RSA database, and assures that all policies and procedures are followed according to the Secure ID Card SOP and processes.

VII. **Document Information**

Initial Issue Date: May 1, 2009
Last Revision Date: January 4, 2016 – To update Document Information.

Point of Contact: Henry Quintal, Architecture-Policy Administrator, OIT, 207-624-8836.
Approved By: Greg McNeal, Chief Technology Officer, OIT, (207) 624-7568.
Enforced By: Greg McNeal, Chief Technology Officer, OIT, (207) 624-7568.

Legal Citation: Title 5, Chapter 163: Office of Information Technology[1]
Waiver Process: See the Waiver Policy[2].

[1] http://legislature.maine.gov/statutes/5/title5ch163sec0.html

[2] http://maine.gov/oit/policies/waiver.htm